

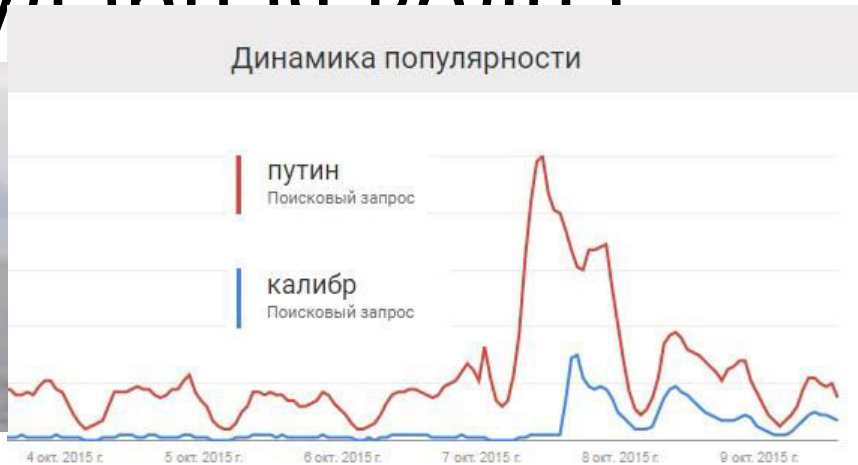
Информационные атаки и защита репутации банка

Технология интернет-разведки Avalanche

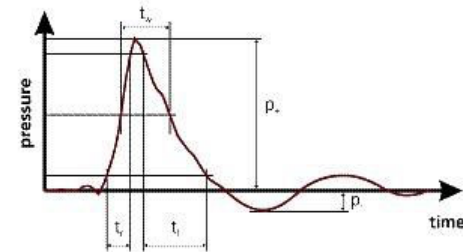
МАСАЛОВИЧ
Андрей Игоревич
avalanche100500@gmail.com
(964) 577-2012



Естественное распространение новости: ударная волна



Ударная волна



Искусственные информационные волны – аналог двумерной волны

- Каждая точка волны может стать
источником новой волны,
давая начало квантовой волно-
вой функции



Пример астротурфинга:
50 лет полета Терешковой



“Sally Ride, the first woman in Space”

Denver Post



Wonderville



Inquisitr



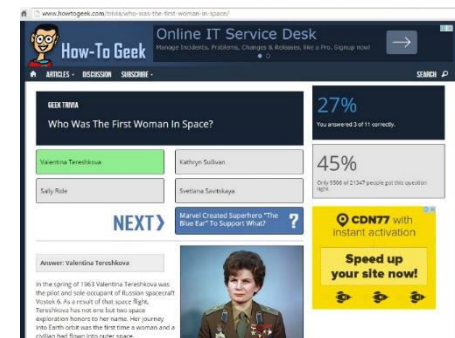
LubbockOnline



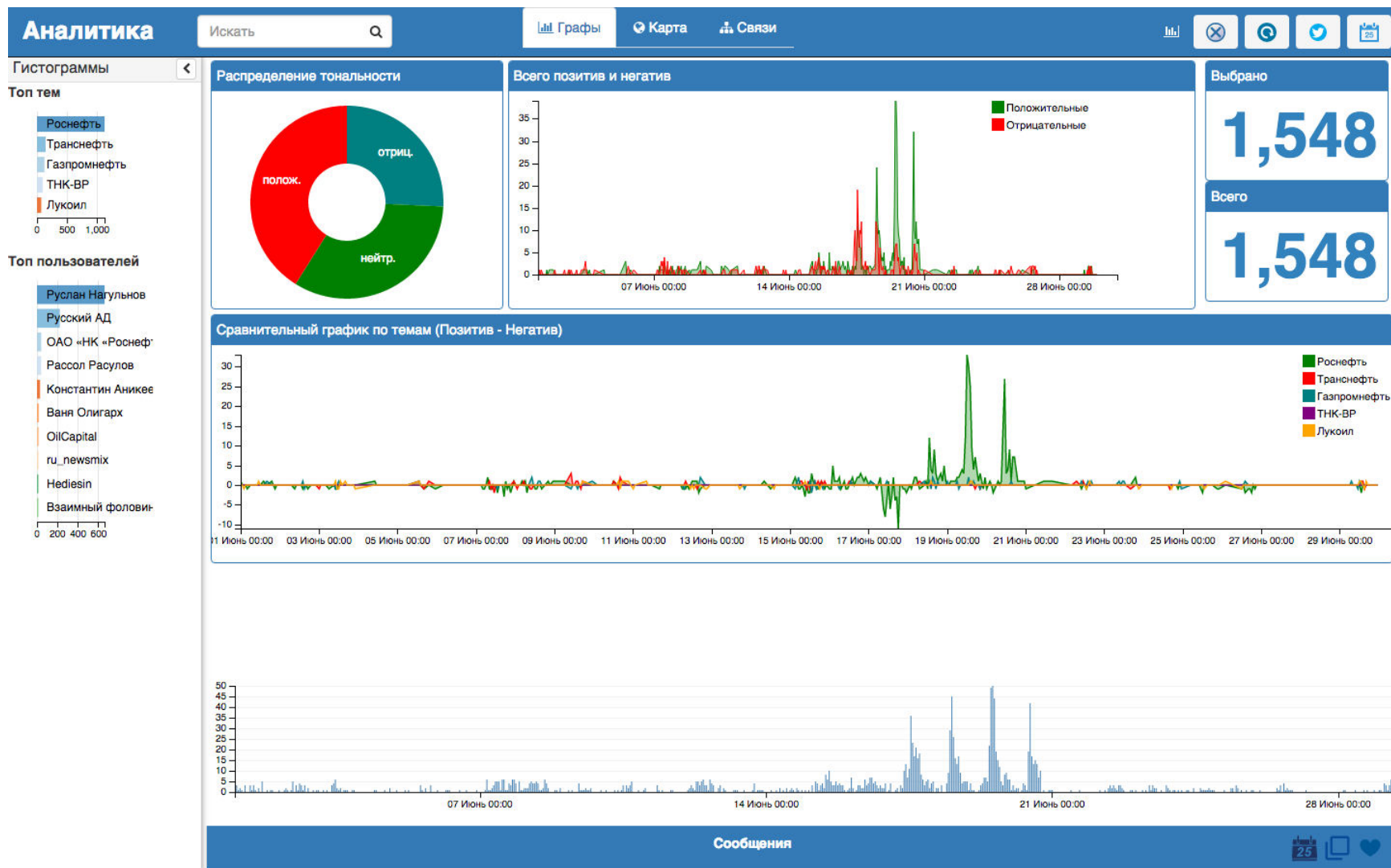
McDonalds



Опрос: Терешкова-45%

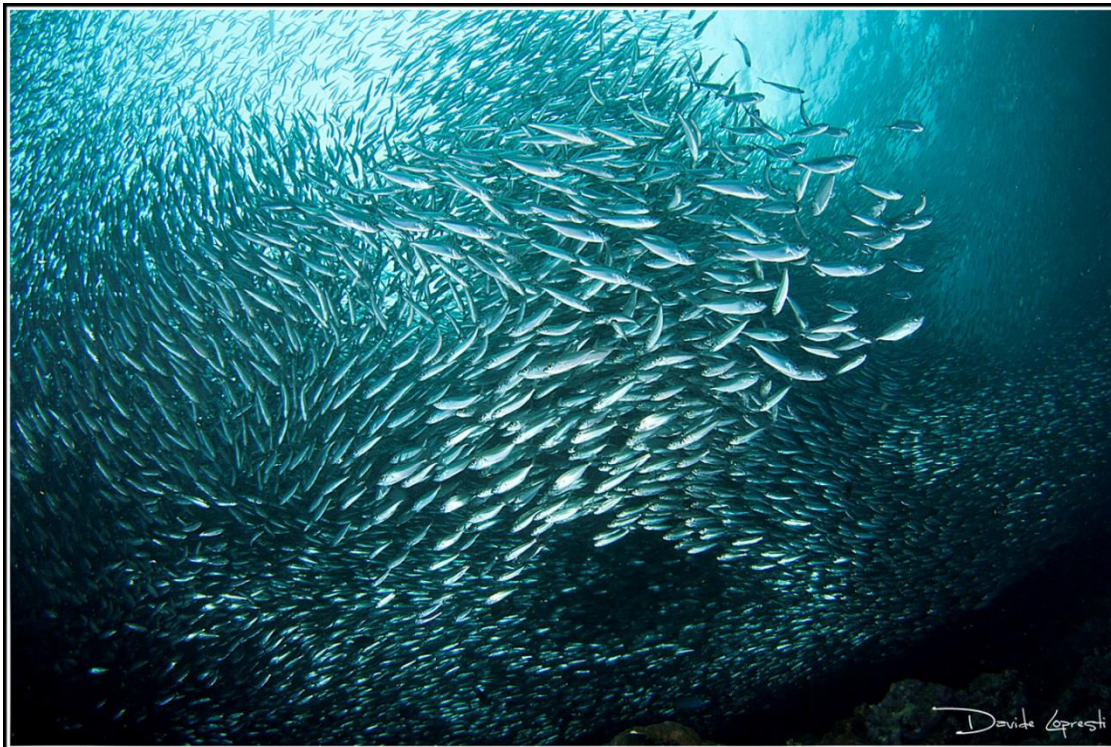


Преимущества технологии Avalanche: Анализ информационных всплесков



Вброс: этапы распространения

- Сначала – сеть подконтрольных ресурсов
- Затем – последователи (followers)
- Далее – очаги возбуждения в среде объектов воздействия



Преимущества технологии Avalanche: Выявление ссылочных взрывов

Яндекс
блоги

#роснефть

в регионе «Москва и Московская область»

Найти

расширенный поиск

Показаны сообщения 51 — 60 из 344 найденных.

 Михаил Леонтьев и **Роснефть** politota.d3.ru/leontev-odnako-lishnego-naboltal-832534/ #однако #леонтьев #роснефть
12 сентября 2015, 14:05 · [margaritka](#)

[Михаил Леонтьев и Роснефть https...](#)
показать полный текст
Михаил Леонтьев и **Роснефть** <https://politota.d3.ru/leontev-odnako-lishnego-naboltal-832534/> #однако #леонтьев #роснефть. однако. леонтьев. **роснефть**.
12 сентября 2015, 13:22 · [Ольга Бергер](#) · www.facebook.com/profile.php?id=100009464359930

 Михаил Леонтьев и **Роснефть** [https...](https://politota.d3.ru/leontev-odnako-lishnego-naboltal-832534/)
показать полный текст
Михаил Леонтьев и **Роснефть** <https://politota.d3.ru/leontev-odnako-lishnego-naboltal-832534/> #однако #леонтьев #роснефть. однако. леонтьев. **роснефть**.
12 сентября 2015, 12:40 · [Фишка Фишка](#) · www.facebook.com/profile.php?id=100004999474368

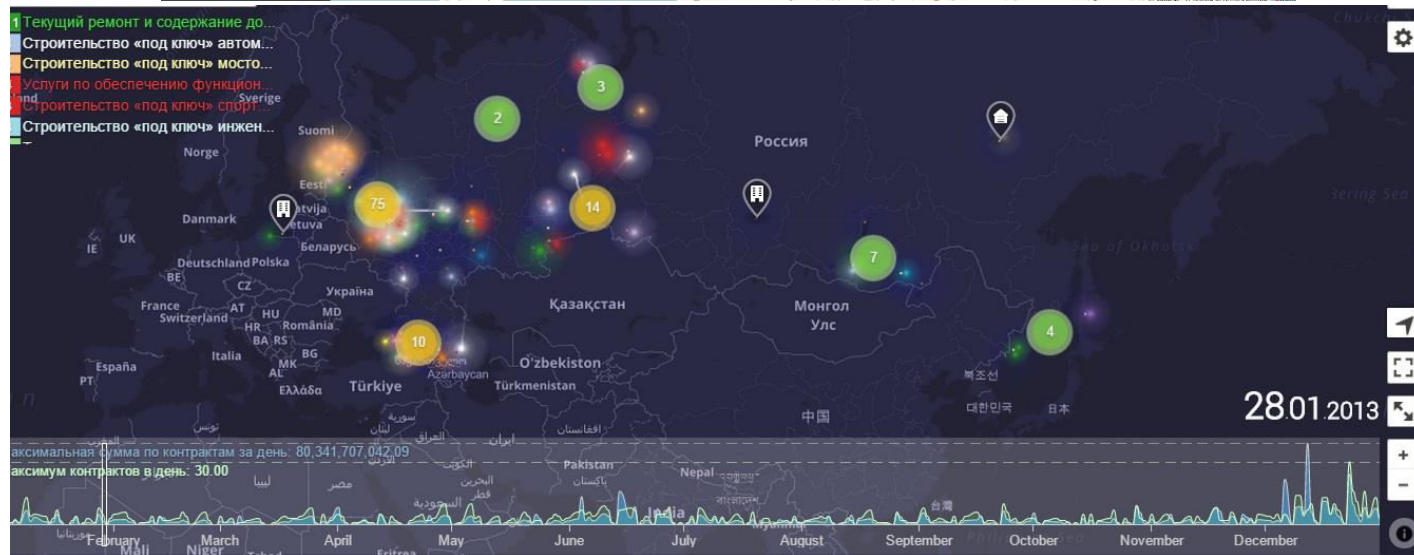
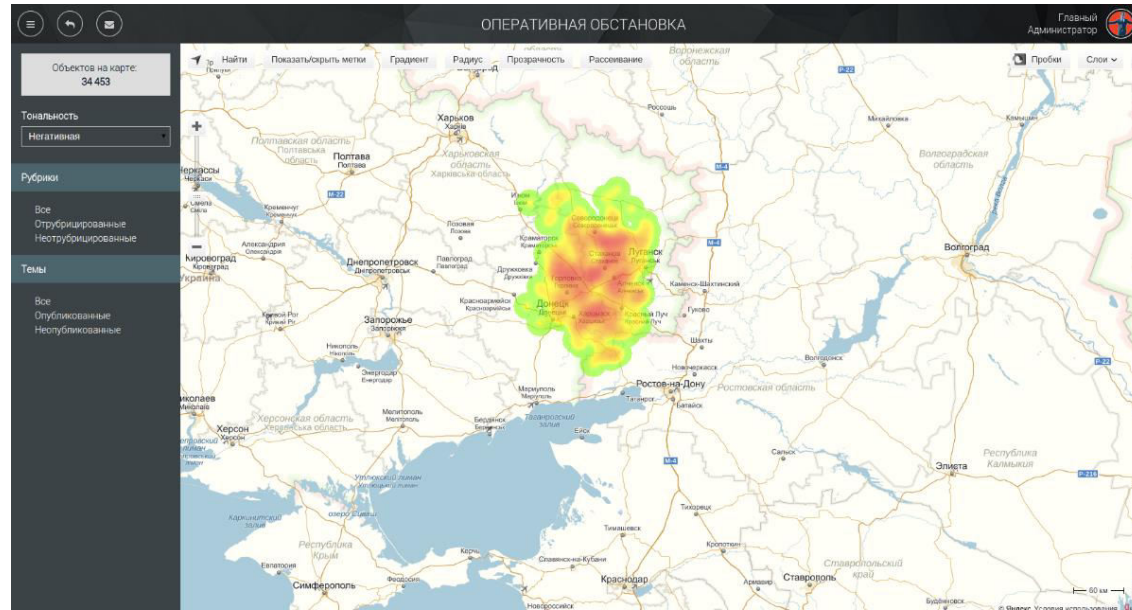
 Михаил Леонтьев и **Роснефть** [https...](https://politota.d3.ru/leontev-odnako-lishnego-naboltal-832534/)
показать полный текст
Михаил Леонтьев и **Роснефть** <https://politota.d3.ru/leontev-odnako-lishnego-naboltal-832534/> #однако #леонтьев #роснефть. однако. леонтьев. **роснефть**.
12 сентября 2015, 12:31 · [Елизавета Елисеева](#) · www.facebook.com/profile.php?id=100008049849611

 Михаил Леонтьев и **Роснефть** [https...](https://politota.d3.ru/leontev-odnako-lishnego-naboltal-832534/)
показать полный текст
Михаил Леонтьев и **Роснефть** <https://politota.d3.ru/leontev-odnako-lishnego-naboltal-832534/> #однако #леонтьев #роснефть. однако. леонтьев. **роснефть**.
12 сентября 2015, 11:08 · [Рома Лугоборский](#) · www.facebook.com/profile.php?id=100005471509501

 Михаил Леонтьев и **Роснефть** [https...](https://politota.d3.ru/leontev-odnako-lishnego-naboltal-832534/)
показать полный текст
Михаил Леонтьев и **Роснефть** <https://politota.d3.ru/leontev-odnako-lishnego-naboltal-832534/> #однако #леонтьев #роснефть. однако. леонтьев. **роснефть**.
12 сентября 2015, 10:52 · [Ольга Милина](#) · www.facebook.com/profile.php?id=100008961787252

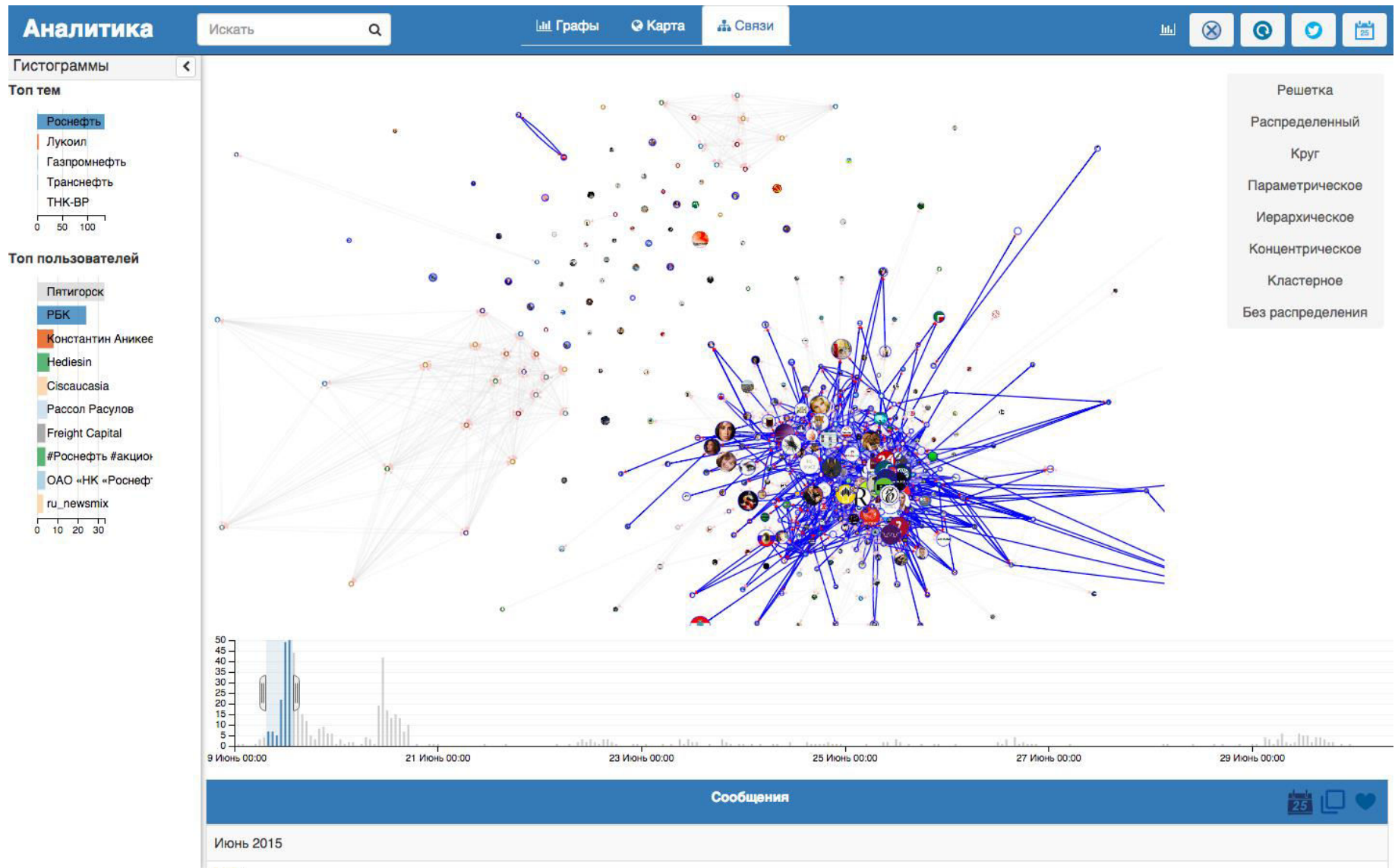
Преимущества технологии Avalanche:

Тепловая карта активности в социальных сетях

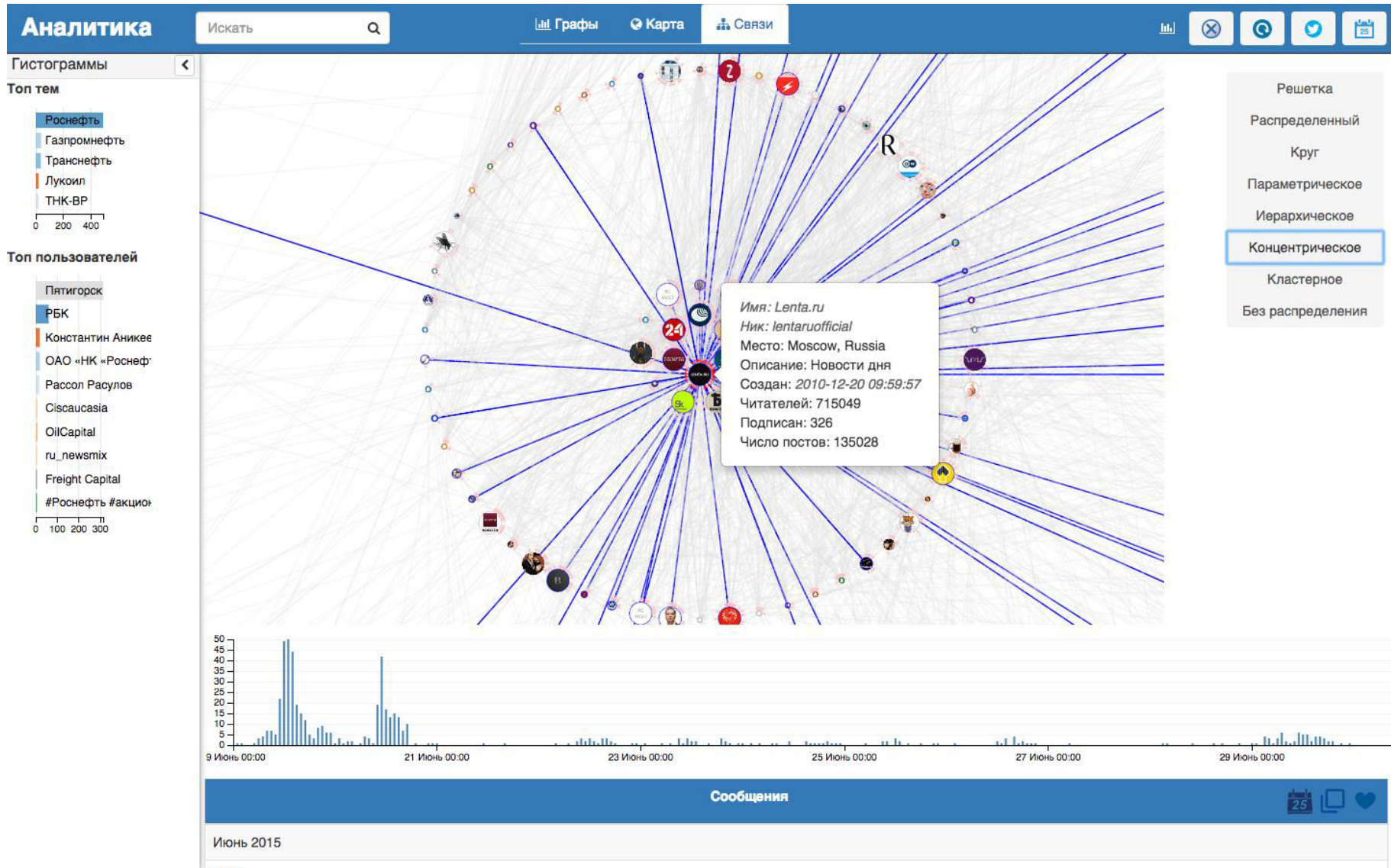


Преимущества технологии Avalanche:

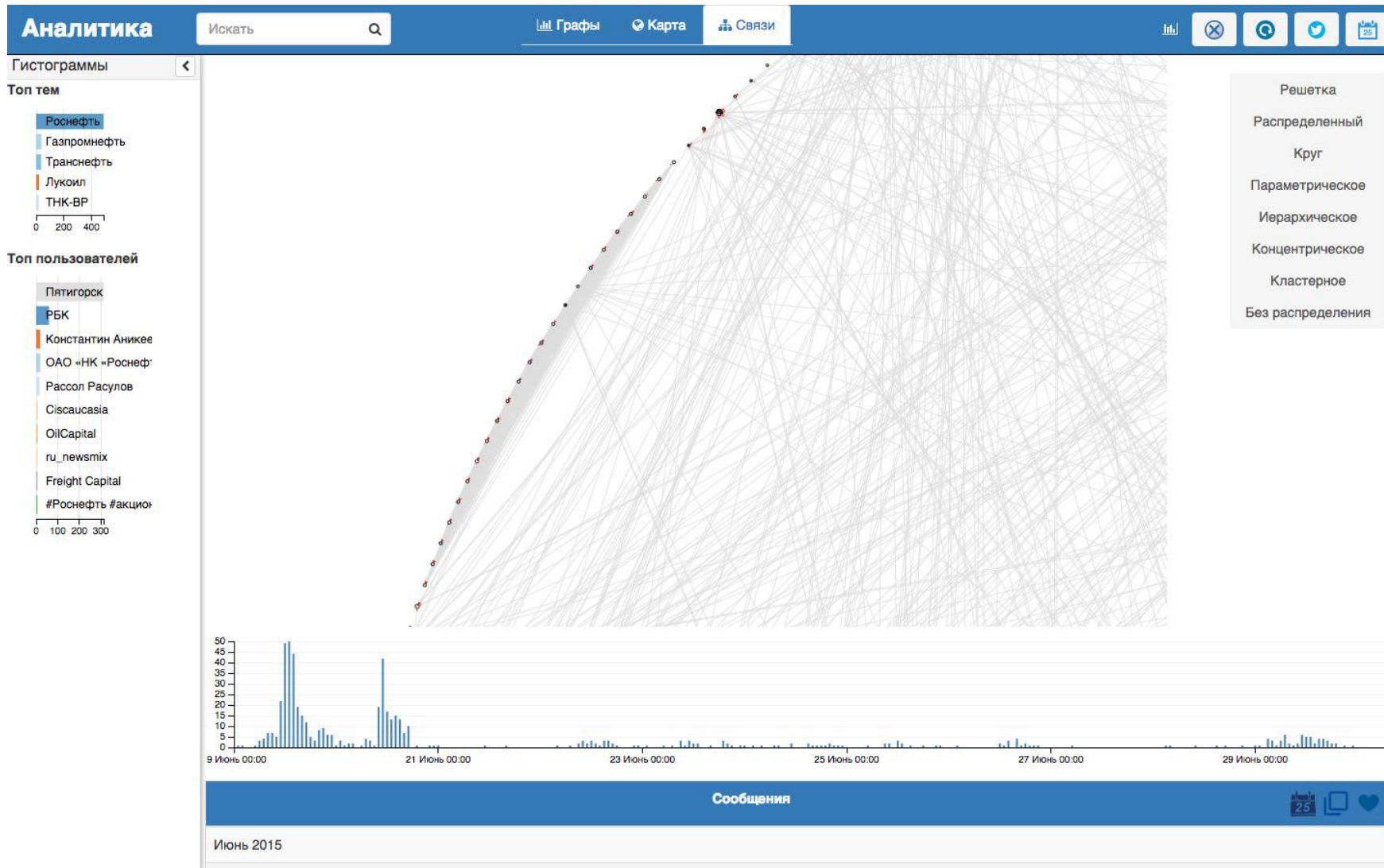
Анализ активности в социальных сетях



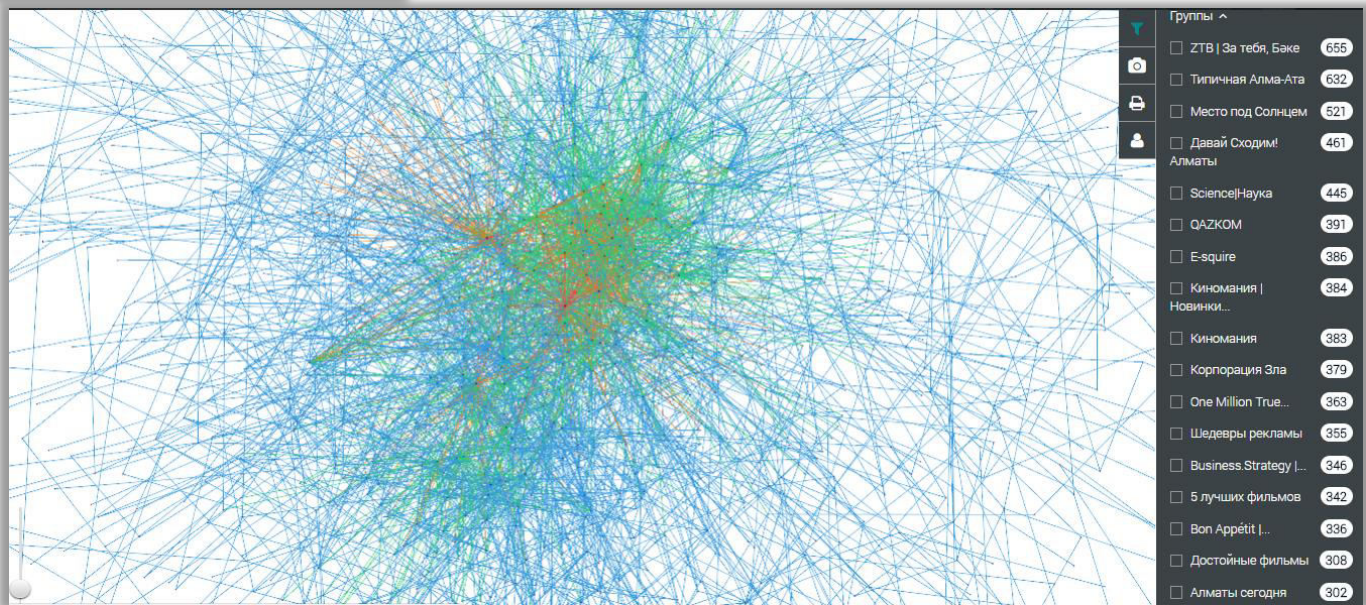
Преимущества технологии Avalanche: Контроль распространения информации



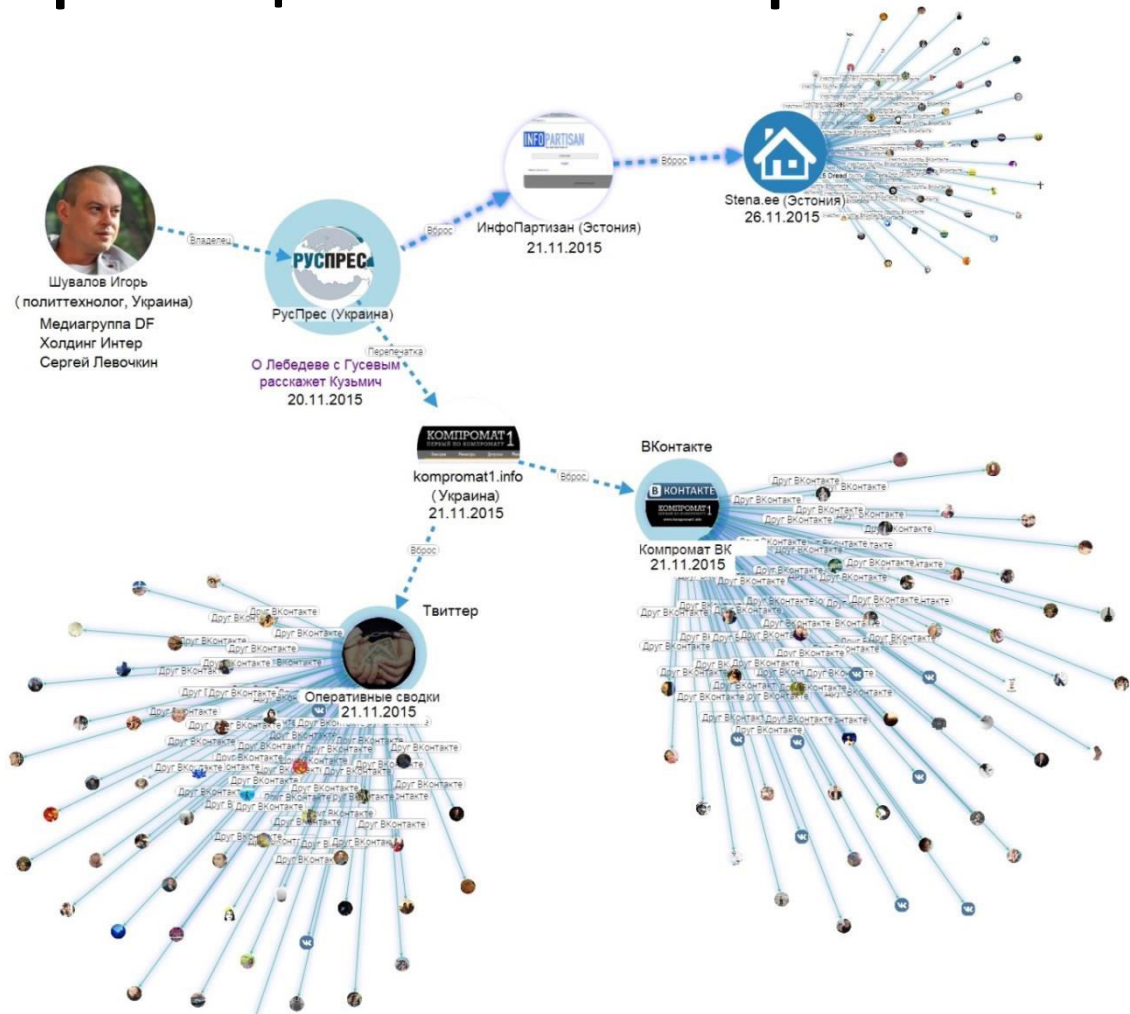
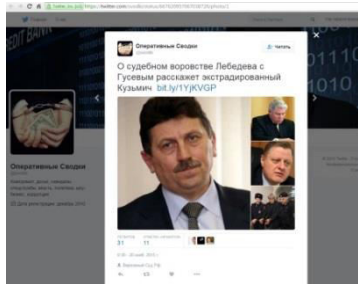
Преимущества технологии Avalanche: Автоматическое выявление ботов



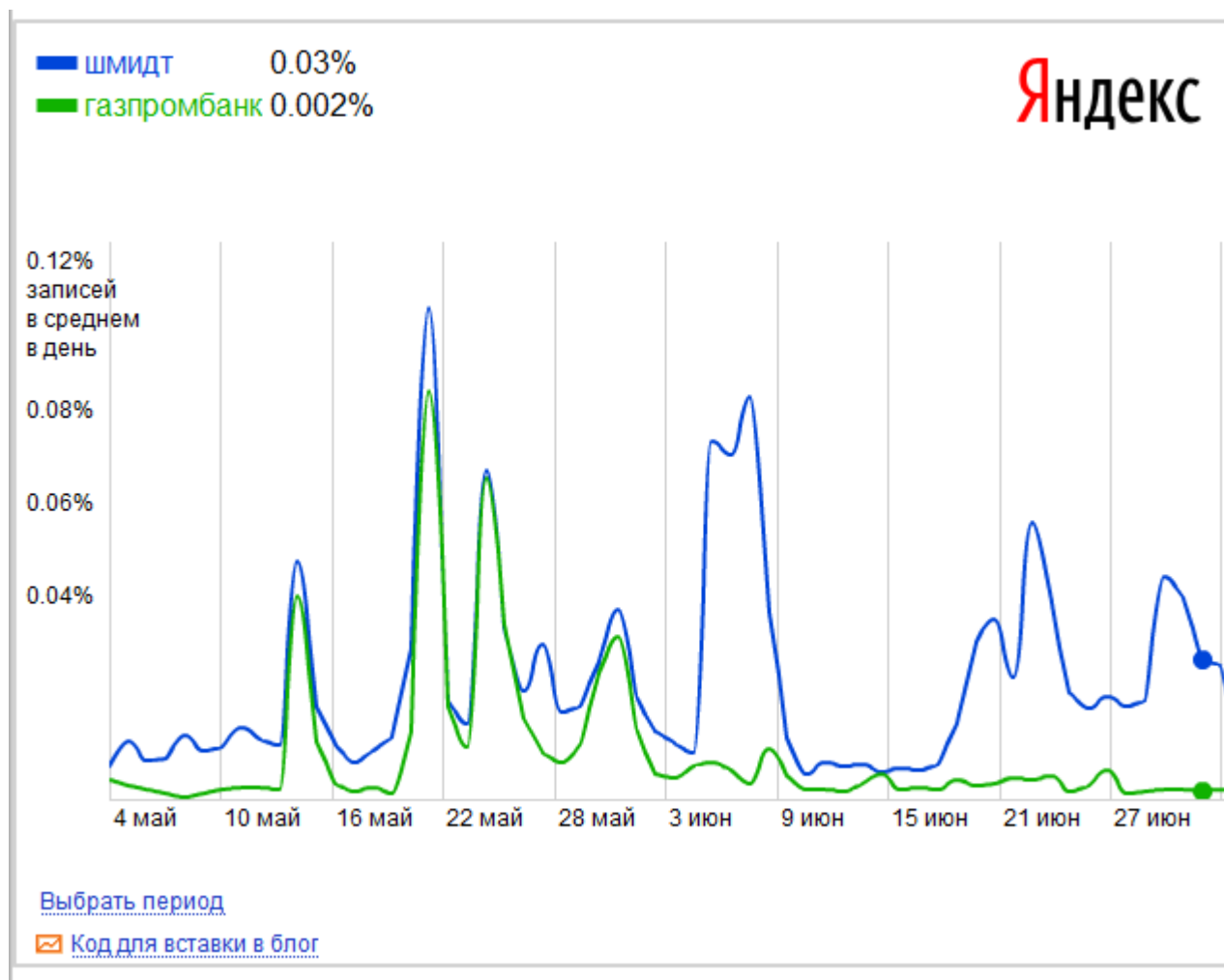
Пример: анализ аудитории Казкоммерцбанка



Анализ источников информационных вбросов



Пример активного противоборства



Пример экрана контроля оперативной обстановки



Первый Галактический Банк

admin

Топ-менеджмент

"Деловой Петербург". Пла...

01.07.2014 21:24:51

Активы обанкротившегося племзавода "Мыслинский", на которые претендует агрохолдинг банкира Андрея Исаева, http://www.dp.ru/a/2014/06/30/Planovoe_bankrotstv

Глава правления банка «С...

20.06.2014 09:00:24

А «Балтийский» банк назначил внеочередное собрание акционеров на 25 августа. <http://topspb.tv/news/news46011/>

Критика/компромат

У Балтийского банка появи...

02.07.2014 10:27:19

У Балтийского банка появились проблемы? <http://www.bolshoyvopros.ru/questions/1040381-u->

Ngina McCormick @caceno...

01.07.2014 22:50:00

Балтийский #банк #выселяют из центра Петербурга: <https://twitter.com/cacenowmyhe/statuses/4839157C>

Мошенничество при кредитовании

Кредит наличными, банк к...

02.07.2014 06:38:20

Кредит наличными, банк кредит, деньги. ДОЛЖНИКАМ И БЕЗРАБОТНЫМ, а так же http://www.zacreditom.ru/board/chastnye_objavlenije

КРЕДИТЫ! ОДОБРЕНИЕ КР...

02.07.2014 02:34:29

Помощь мгновенная, оперативная, без денег не отпустим! http://www.zacreditom.ru/board/chastnye_objavlenije

Банк в регионах

Юрисконсульт

29.06.2014 22:53:00

2008-09 г. Консультант ЗАО «Балтийский Банк» г. Санкт - Петербург http://www.avito.ru/mineralnye_vody/rezume/yuriskc

Реферат: Анализ деятельн...

29.06.2014 20:09:32

Автор: Неизвестен (1 стр.)
Название: Анализ деятельности
Управления кредитования Псковского
http://text.tr200.biz/referat_bankovskoe_delo/?

Карточный фрод

Делаю заливов на ваши ка...

02.07.2014 11:08:19

Делаю заливов на ваши карты, суммы разные. Проблем с локами бывает редко: obnal.vs@gmail.com http://www.zacreditom.ru/board/chastnye_objavlenije

ЗАЛИВ НА КАРТУ

02.07.2014 08:50:07

ЛЮДИ!!! Вы не все что-ли еще подарили денег кидалам типа АТМ и ЗАЛИВЩИК??? 1. НИКОГДА http://www.zacreditom.ru/board/chastnye_objavlenije

Фрод в ДБО

Обналичивание подвергли...

02.07.2014 00:46:13

Мосгорсуд вчера не смог решить вопрос о продлении срока содержания под стражей бизнесмена <http://www.kommersant.ru/doc/2503570>

Хакеры идут: "русскоговор...

01.07.2014 18:10:14

"Салли Скатт, заместитель главного управляющего Британской ассоциации банкиров, сказала на той же <http://inopressa.ru/article/01Jul2014/inopressa/hacke>

Инциденты ИБ в банках

Уязвимость 86% Android-y...

02.07.2014 09:00:00

Глава отдела Security Research Group компании IBM Рои Хэй заявил об уязвимости в сервисе Android KeyStore, <https://xakepy.cc/content.php?r=6772->

Дело банкира Гительсона ...

01.07.2014 22:28:01

В Петербурге перед судом предстанет бывший председатель совета директоров ОАО «Банк ВЕФК» и ОАО <http://www.fontanka.ru/2014/07/01/022/>

Утечки информации, уязвимости

Сайт: baltleasing.ru

02.07.2014 07:46:40

обнаружены проблемы безопасности <http://www.webbez.ru>

Сайт: baltleasing.ru

02.07.2014 07:46:40

обнаружены проблемы безопасности <http://www.webbez.ru>



Технология **Avalanche** – интернет-разведка в арсенале Ситуационных центров

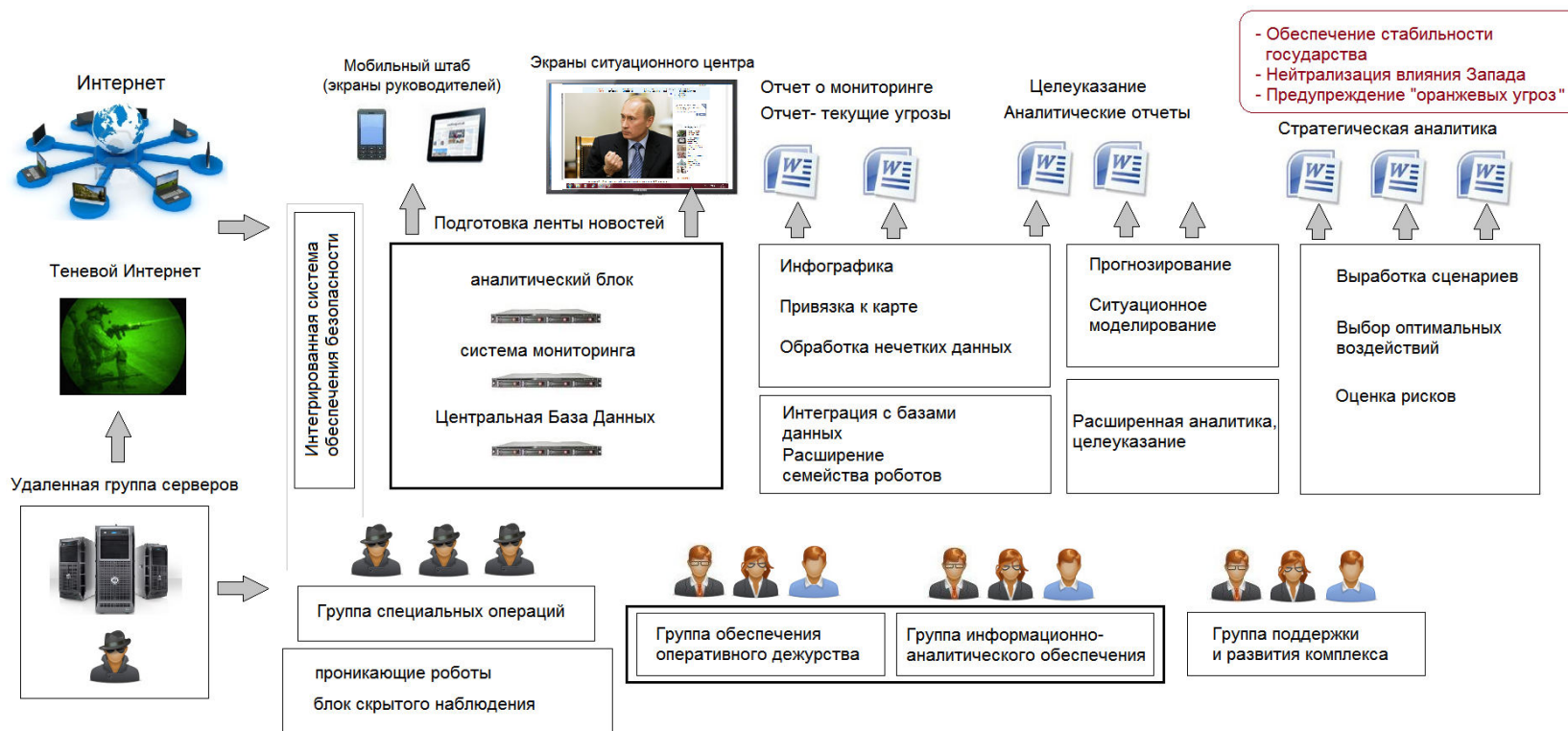
- Технология разработана более 10 лет назад
- Комплекс интернет-разведки и мониторинга
- Более 20 типов поисковых роботов
- Контроль «серого» (глубинного) Интернета
- Автоматические «светофоры» уровня угроз
- Раннее обнаружение информационных атак



АВАЛАНЧ

Технологическая платформа информационного противоборства

Структура программного обеспечения Ситуационного центра



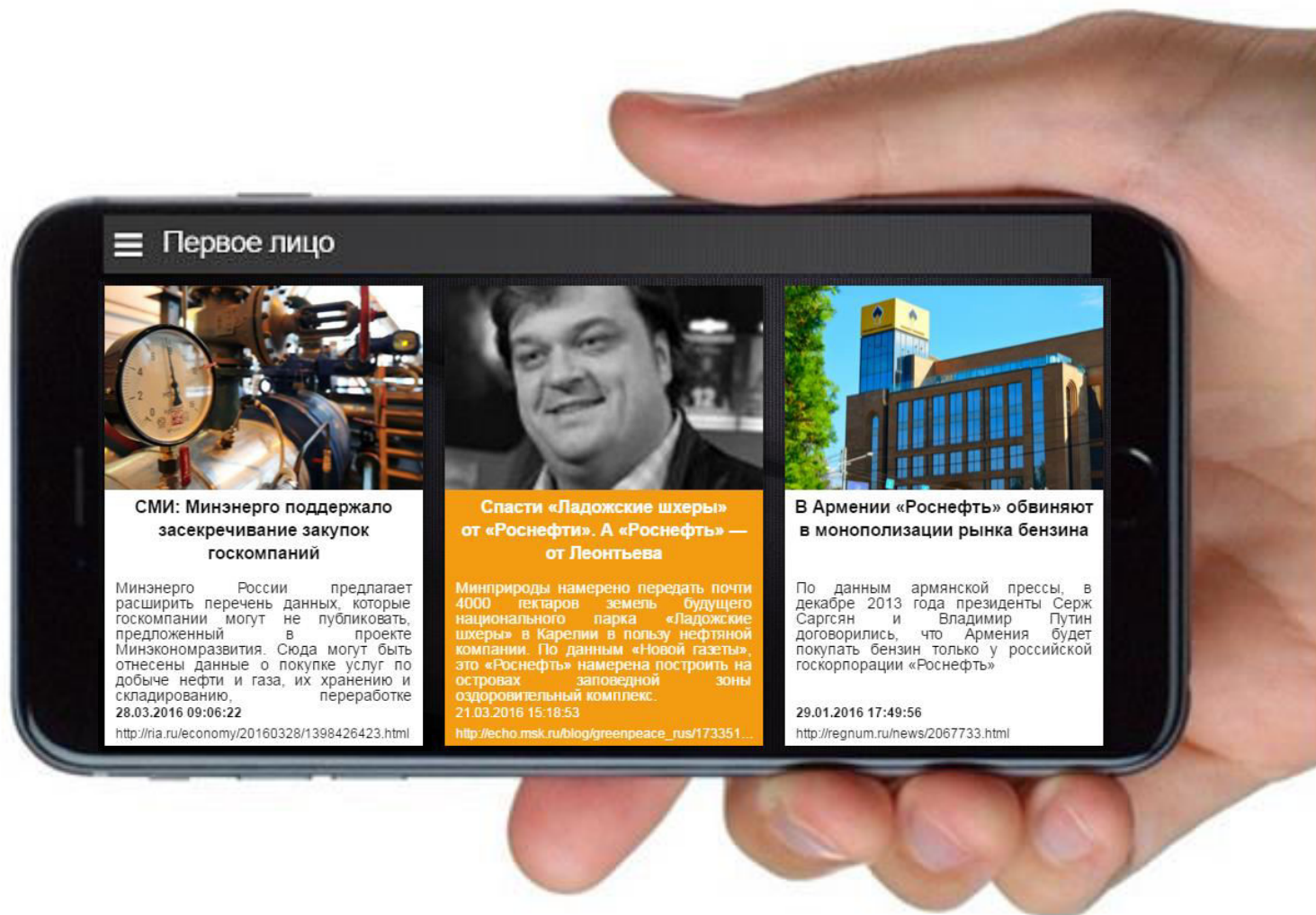
Цели развертывания комплекса

- Информационное обеспечение Руководства
- Раннее обнаружение угроз бизнесу, репутации и устойчивому развитию
- Мониторинг активности и выявление информационных атак в социальных сетях;
- Противодействие недобросовестной конкуренции;
- Контроль защищенности собственных информационных ресурсов;

Проблемы, которые выявляет комплекс

- Угрозы бизнесу, репутации, устойчивому развитию
- Критика, компромат, негатив в адрес банка
- Утечки коммерческой тайны, конфиденциальной и внутренней информации
- Утечки персональных данных
- Конфликты интересов банка и его менеджмента
- Риски проникновения в банк криминальных элементов
- Недобросовестная конкуренция
- Противоправные действия менеджмента
- Новые схемы мошенничества, фрода в ДБО и др.
- И т.д.

Преимущества технологии Avalanche: Экран руководителя - планшет и смартфон



☰ Первое лицо



**СМИ: Минэнерго поддержало
засекречивание закупок
госкомпаний**

Минэнерго России предлагает расширить перечень данных, которые госкомпании могут не публиковать, предложенный в проекте Минэкономразвития. Сюда могут быть отнесены данные о покупке услуг по добыче нефти и газа, их хранению и складированию, переработке

28.03.2016 09:06:22

<http://ria.ru/economy/20160328/1398426423.html>



**Спасти «Ладожские шхеры»
от «Роснефти». А «Роснефть» —
от Леонтьева**

Минприроды намерено передать почти 4000 гектаров земель будущего национального парка «Ладожские шхеры» в Карелии в пользу нефтяной компании. По данным «Новой газеты», это «Роснефть» намерена построить на островах заповедной зоны оздоровительный комплекс.

21.03.2016 15:18:53

http://echo.msk.ru/blog/greenpeace_rus/173351...



**В Армении «Роснефть» обвиняют
в монополизации рынка бензина**

По данным армянской прессы, в декабре 2013 года президенты Серж Саргсян и Владимир Путин договорились, что Армения будет покупать бензин только у российской госкорпорации «Роснефть»

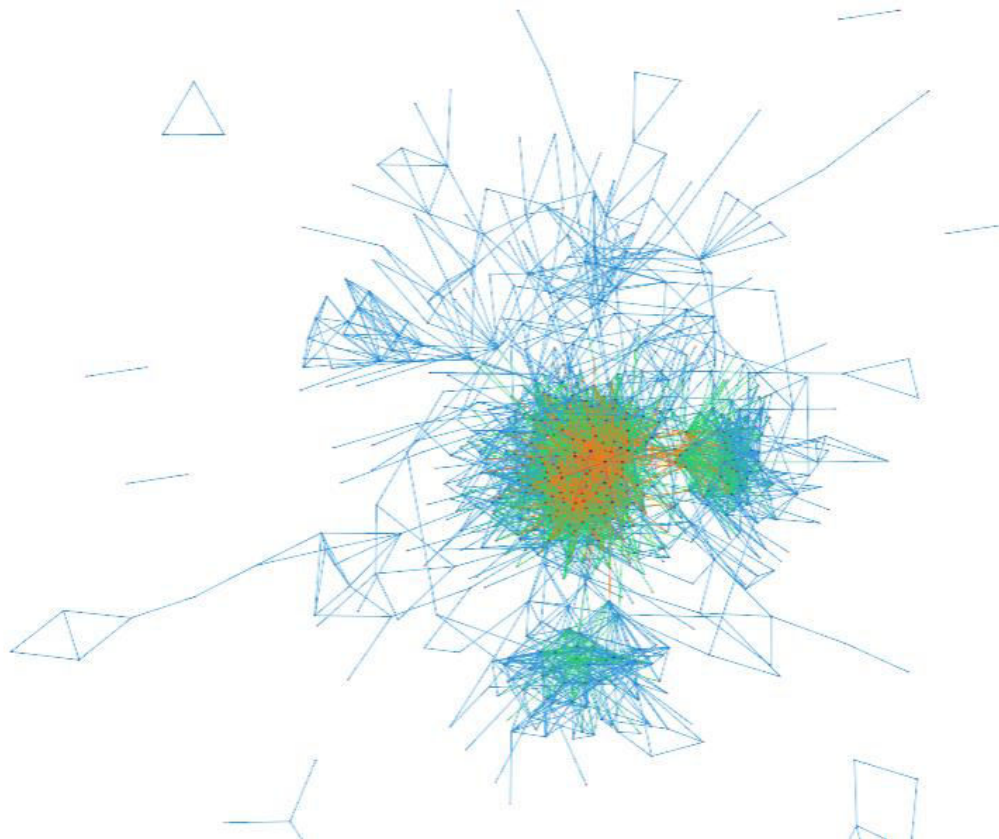
29.01.2016 17:49:56

<http://regnum.ru/news/2067733.html>

Преимущества технологии Avalanche:

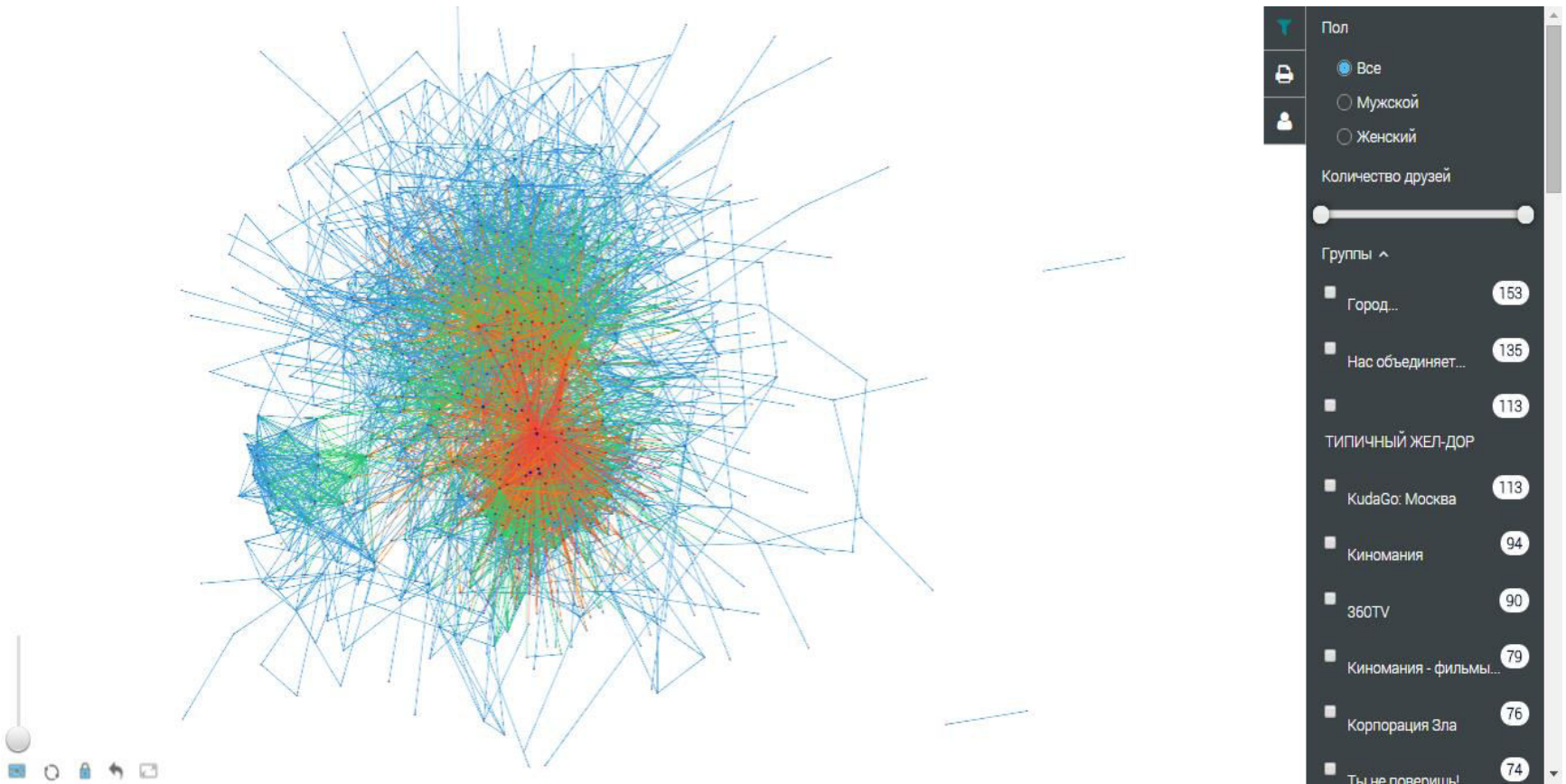
Построение социальных портретов

Пример: связи и интересы топ-менеджера

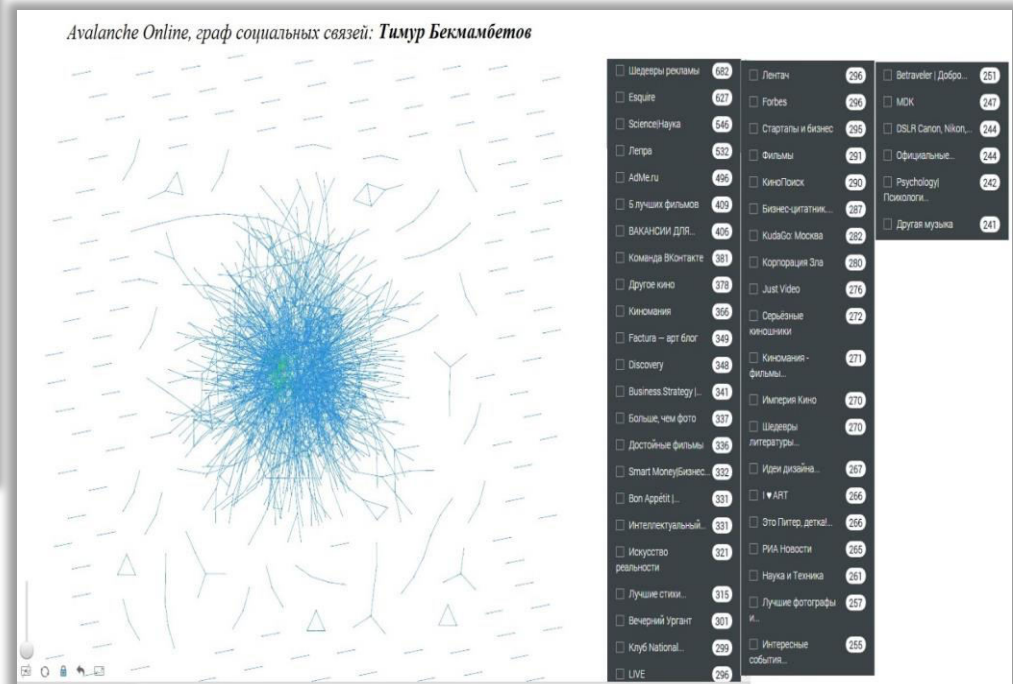
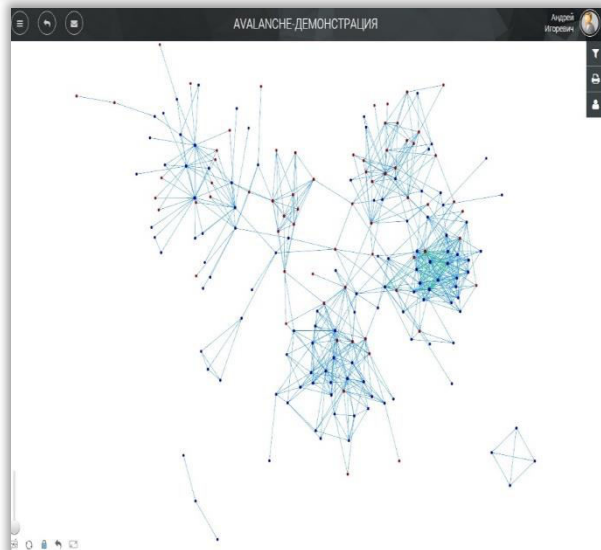
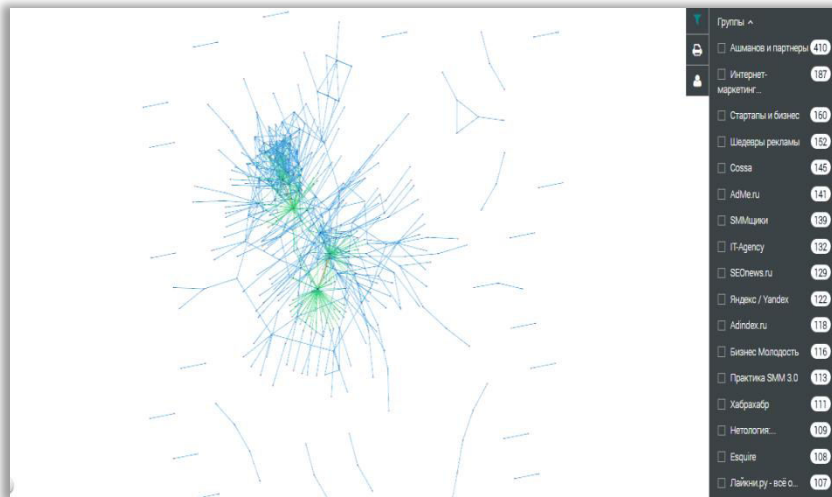


Группы ^	
■ KudaGo: Москва	80
■ Интересная Москва	69
■ 360TV	64
■ Город...	64
■ Шедевры рекламы	52
■ Киномания	50
■ ВАКАНСИИ ДЛЯ...	49
■ Crazy salsa - школа...	49
■ Лепра	45
■ Science Наука	45
■ Esquire	41
■	41
■ РИАМО в Подмосковье	41

Социальный портрет - политик



Социальный портрет – блогер



Краткие результаты тестирования информационно-поисковой системы «Лавина Пульс»

Лавина Пульс – система контроля оперативной обстановки в Сети

Система Лавина Пульс объединяет в себе расширенные возможности интернет-поиска (на основе собственного семейства поисковых роботов) и средства автоматизированного ведения досье с возможностями интеллектуальной аналитической обработки больших данных (Big Data) и выявления актуальных угроз в сети Интернет и социальных сетях (слухи о предстоящем банкротстве банков, компромат и т.п.), которые могут привести к возникновению репутационных рисков и проблемам с устойчивостью участников банковского сектора.

Преимущества системы Лавина Пульс

1. Обнаружение угроз на ранних стадиях

- Пример: Утечка информации в Банке России (сентябрь 2015)
- Одной из наиболее громких тем обсуждения в СМИ стала утечка информации об изменении ключевой ставки рефинансирования Банком России в сентябре 2015 года. Ряд СМИ опубликовал информацию об изменении ставки рефинансирования до официального решения Центробанка, что в значительной степени повлияло на ход торгов на финансовых рынках.
- Система Лавина Пульс позволила моментально отслеживать распространение информации в СМИ и реагировать на соответствующие публикации максимально оперативно, на ранней стадии.



Преимущества системы Лавина Пульс

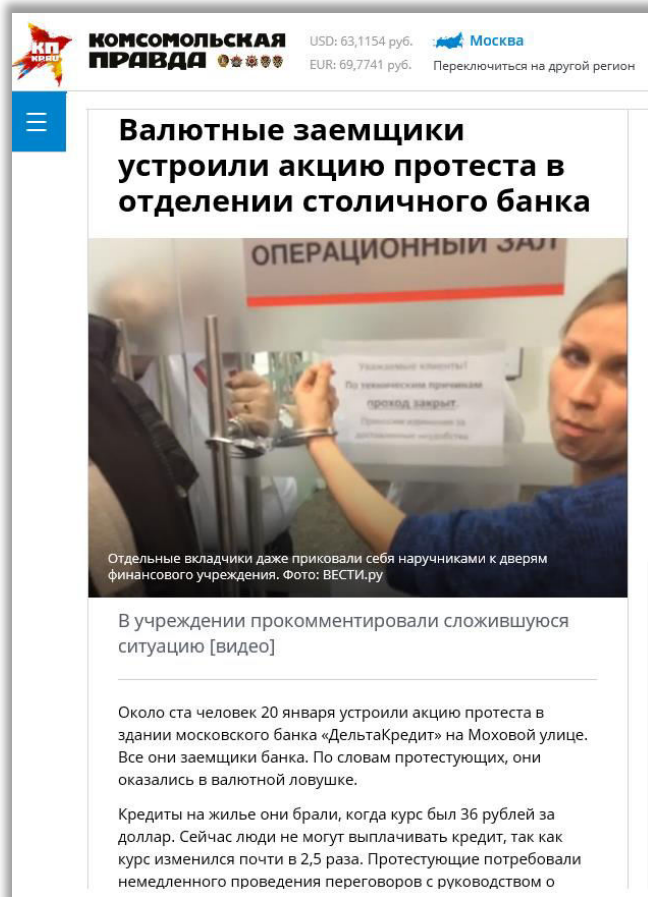
1. Обнаружение угроз на ранних стадиях

- Пример: Акции протеста клиентов «Байкал-банка»
- Система Лавина Пульс следит за информационным фоном вокруг проблемных банков и на ранних стадиях оповещает о возможных проблемах, в том числе реакции жителей на его закрытие, а также предоставляет информацию по поведению вкладчиков.



2. Раннее обнаружение резонансных тем.

- Пример: Акции протеста валютных заемщиков (20.01.2016)
- Изначально, после ослабления курса рубля, активность валютных заемщиков началась в социальных сетях, затем – разовые выступления, и только после этого волна была подхвачена федеральными и региональными СМИ.
- Система Лавина Пульс позволила идентифицировать угрозу еще на уровне социальных сетей и региональных СМИ, задолго до того, как история получила федеральное освещение.



Преимущества системы Лавина Пульс

3. Обнаружение утечек внутренней и конфиденциальной информации, персональных данных и др. с выявлением первоисточника утечки.

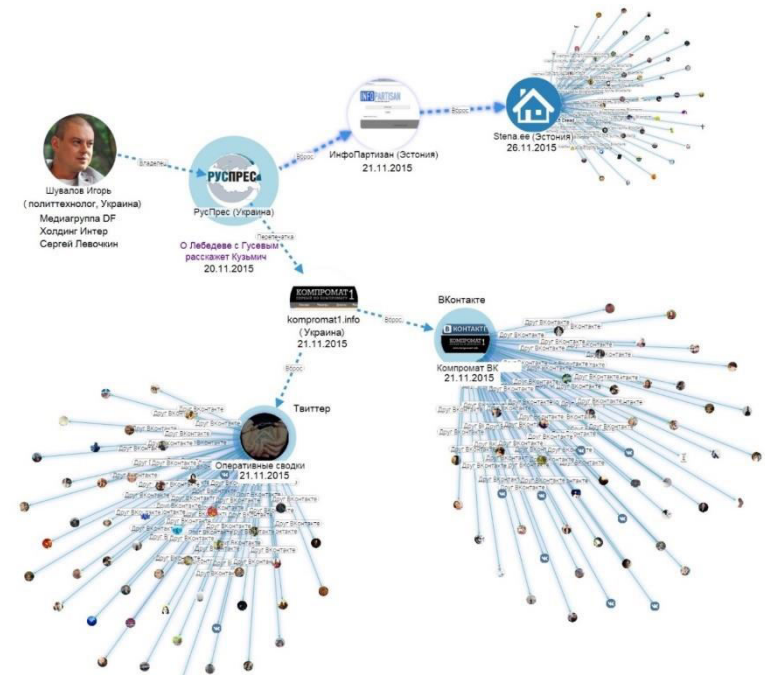
- Специализированные роботы системы Лавина Пульс автоматически обнаруживают утечки секретной, конфиденциальной и внутренней информации, а также персональных данных и коммерческой тайны
- Пример: разглашение персональных данных в документе «Годовой отчет Банк России» ДНК «Доступное жилье»

dsk.vrn.ru/wp-content/uploads/2015/02/Godovoj-otchet-bank-Rossii.pdf

1.14.4	Фактический адрес филиала : нет
1.14.5	Фамилия, имя, отчество руководителя филиала : нет
1.14.6	Номера телефонов филиала : нет
1.14.7	ИНН филиала: нет
1.14.8	КПП филиала: нет
1.14.9	ОГРН филиала: нет
2. Сведения о лицах, входящих в состав органов кооператива	
Исполнительный орган кооператива	
2.1	Должность: Директор
2.2	Фамилия, имя, отчество Образцов Роман Иванович
2.3	Паспортные данные: Паспорт гражданина РФ
2.3.1	Серия: 20 14
2.3.2	Номер: 762638
2.3.3	Дата выдачи: 07.07.2014
2.3.4	Кем выдан: Отделом УФМС России по Воронежской области в Коминтерновском районе г. Воронежа
2.3.5	Код подразделения: 360-004
2.4	ИНН (при наличии): 366605739147
Ревизор кооператива	
2.1	Фамилия, имя, отчество Музылева Елена Николаевна
2.2	Паспортные данные: Паспорт гражданина РФ
2.2.1	Серия: 20 10
2.2.2	Номер: 336772
2.2.3	Дата выдачи: 12.01.2011
2.2.4	Кем выдан: Отделением УФМС России по Воронежской области в Семилукском районе

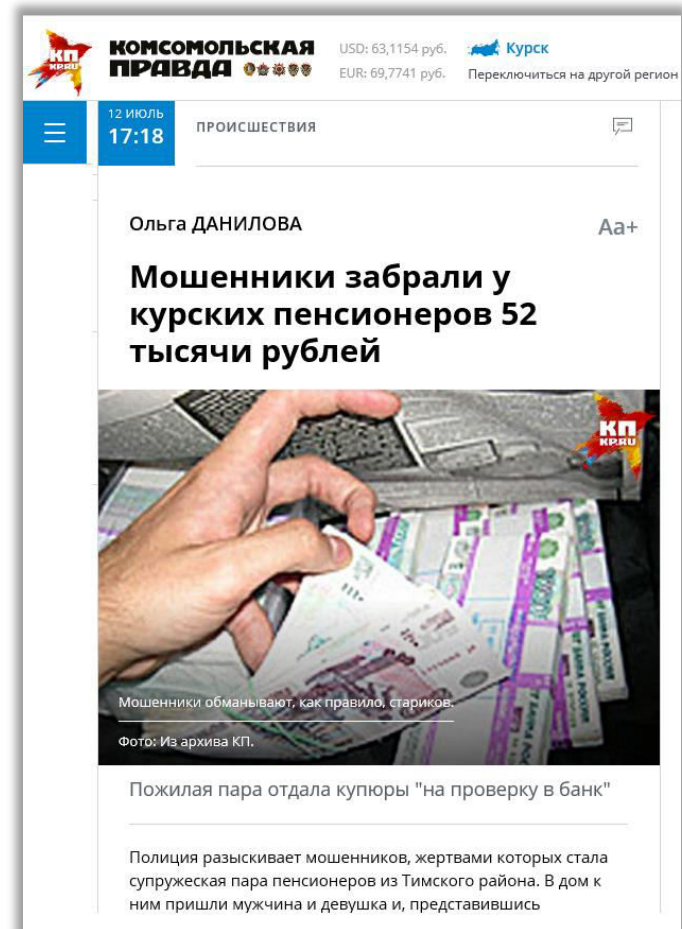
4. Анализ путей распространения информации

- Пример: информационная атака на руководство Верховного суда РФ (сентябрь-октябрь 2015)
- Система Лавина Пульс позволила не только мгновенно получать информацию о новостных вбросах, но и отследить динамику информационных сообщений вплоть до источника.



5. Выявление признаков противоправной деятельности в сети

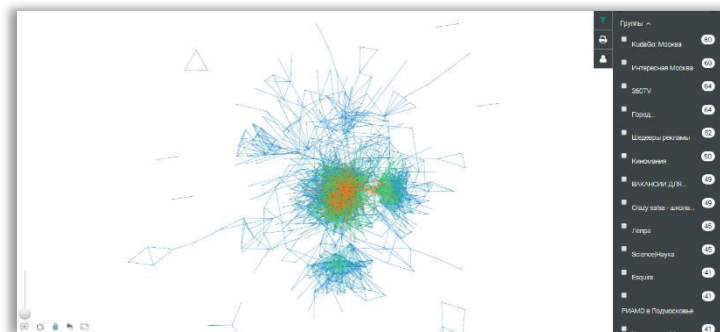
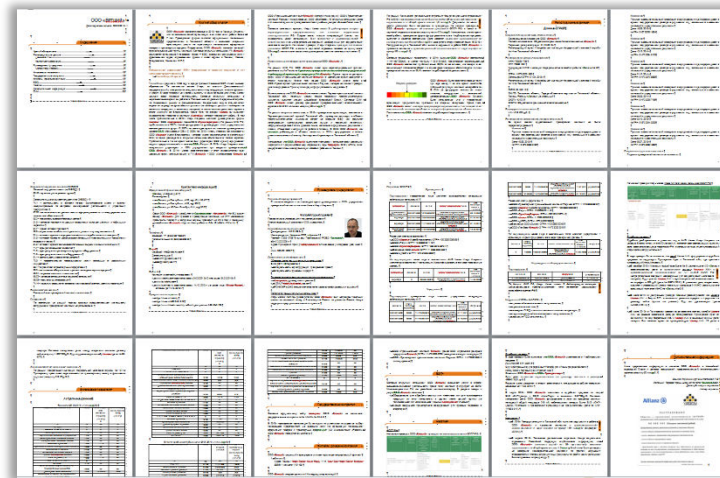
- Пример: в июне 2016 г в Курске мошенники под предлогом подготовки денежной реформы похитили сбережения у нескольких пенсионеров
- Система Лавина Пульс зафиксировала появление и распространение мошеннической схемы задолго до официального пресс-релиза МВД



Преимущества системы Лавина Пульс

6. Сбор досье на объекты интереса

- Система Лавина Пульс позволяет формировать справки и пополнять досье на объекты интереса – организации и персоны
- Сбор информации происходит как из баз данных, так и из различных интернет-источников, включая социальные сети
- Система также строит «социальные портреты» сетевой активности интересующих персон



Преимущества системы Лавина Пульс

7. Тепловые карты общей обстановки

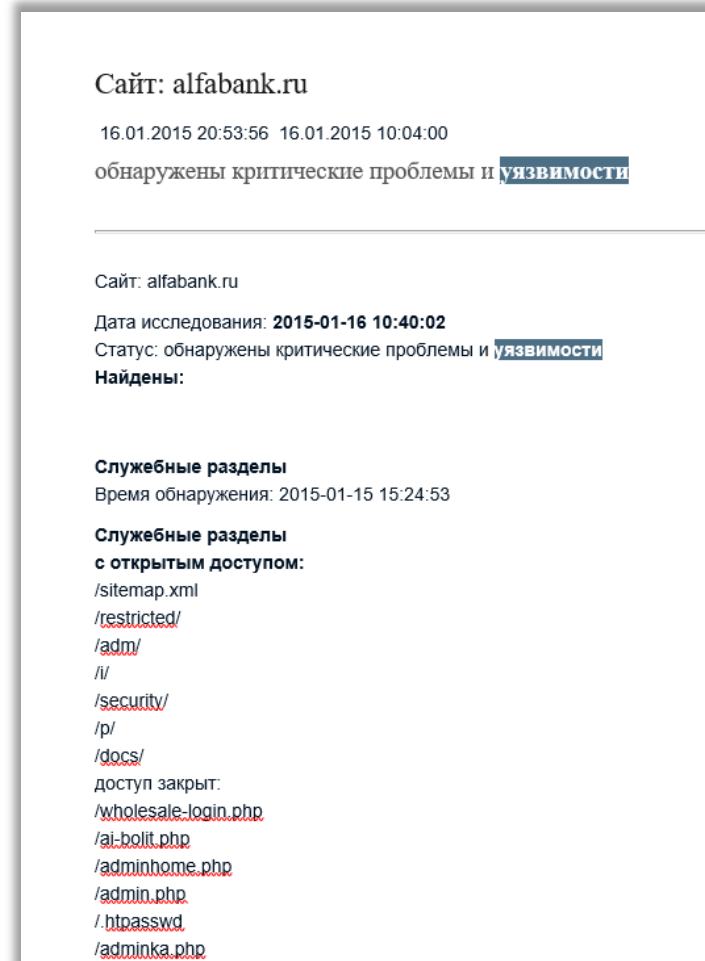
- Система Лавина Пульс позволяет строить «тепловые карты» активности в социальных сетях по заданным темам
- Пример: в декабре 2014 года по России массово распространялись слухи о проблемах со счетами и картами Сбербанка
- Система Лавина Пульс помогла Сбербанку взять ситуацию под контроль



Преимущества системы Лавина Пульс

8. Сканеры защищенности

- В состав Лавина Пульс входит семейство сканеров защищенности, которые постоянно анализируют стойкость заданных интернет-ресурсов к различным видам хакерских атак
- В системе более 60 сканеров
- *Пример: результаты сканирования портала Альфа-банка*



Выводы и рекомендации

По результатам проведённого тестирования
системы «Лавина Пульс»
установлено следующее:

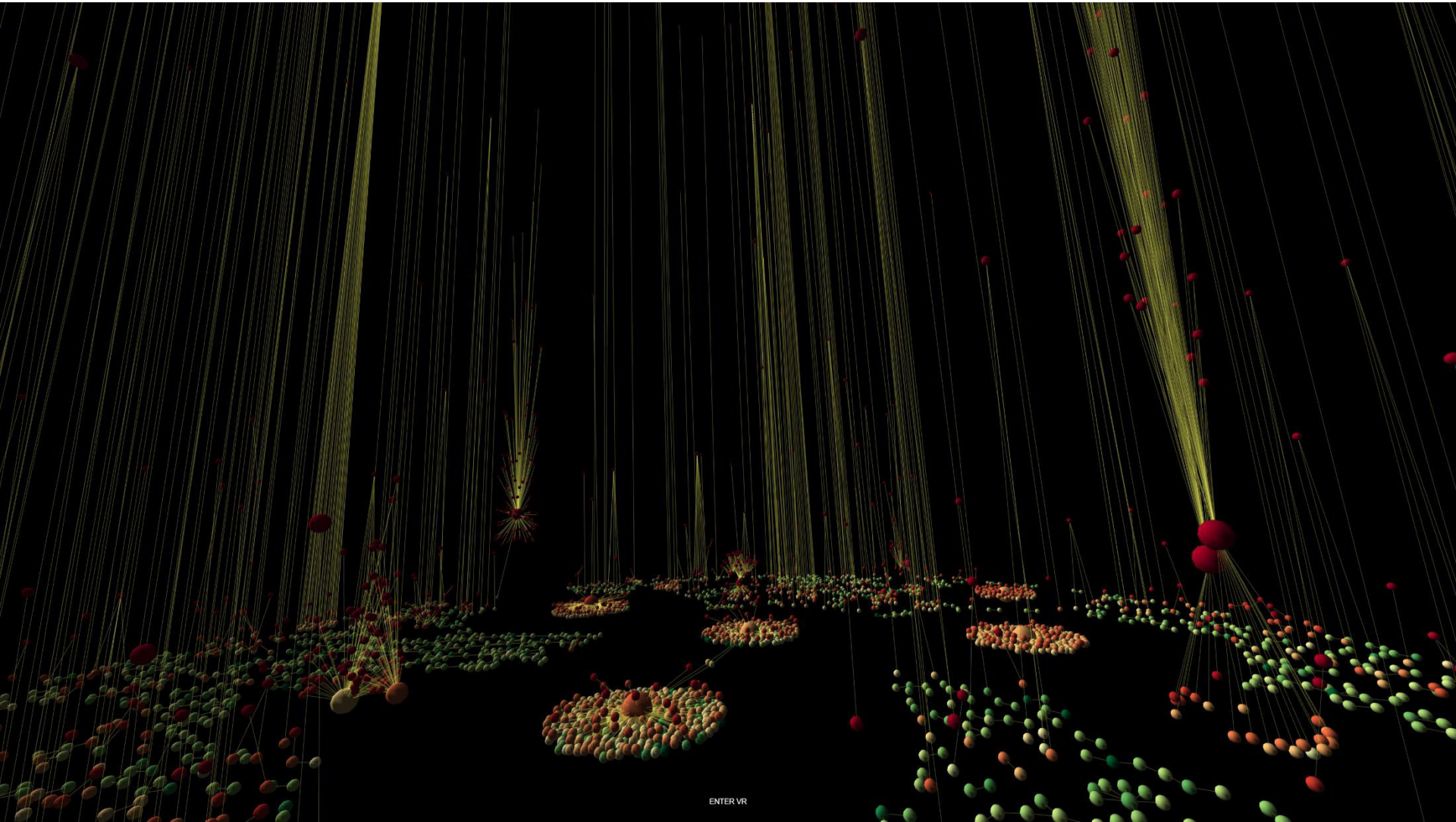
1. Все функции системы Лавина Пульс, заявленные в эксплуатационной документации и проверенные в ходе тестирования полностью реализованы.
2. Система Лавина Пульс в ходе тестирования зарекомендовала себя как инструмент выполнения информационно-аналитической работы и может быть рекомендована к использованию в Банке России

Step to the Web



AVALANCHE

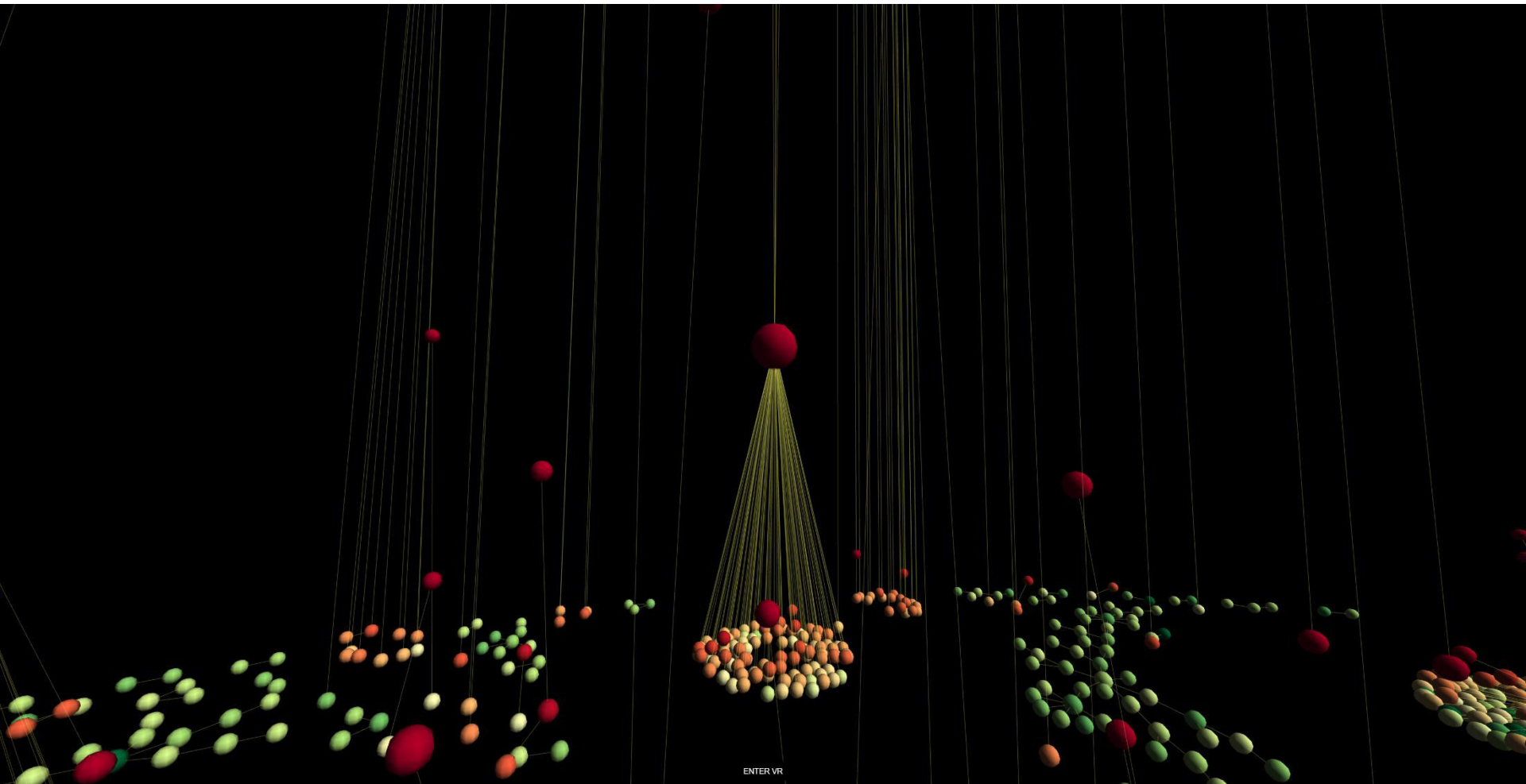
One minute inside Twitter



ENTER VR

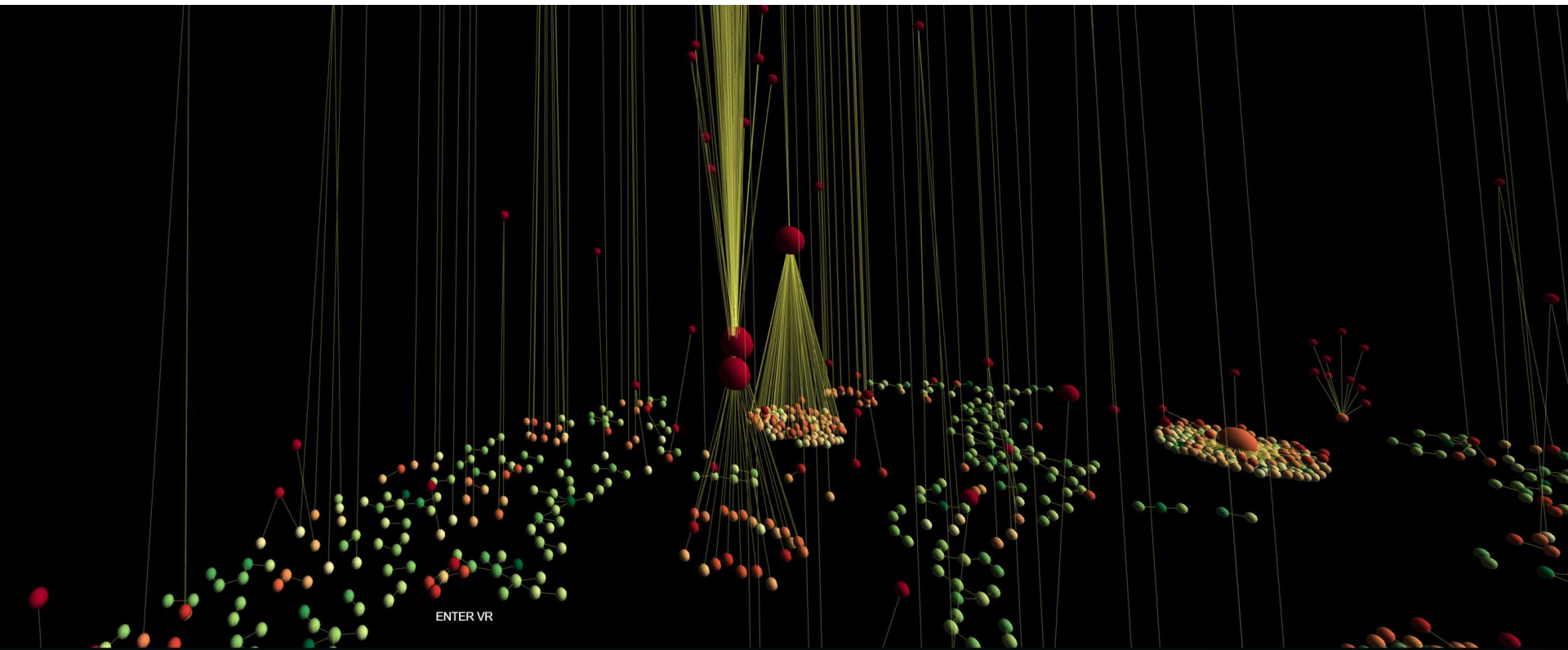
^ V ^ L ^ N C H E

The Leader



^ V ^ L ^ N C H E

Real People vs Botnets



^ V ^ L ^ N C H E

Елки-5: Боты против пиратов

В день выхода фильма «Елки-5» злоумышленники организовали массированное распространение ссылок на пиратскую копию фильма



Противодействие:

- «Поглощение» атаки
- Встречная атака
- «Бот-юрист»

Пожар в Оптиной пустыни: Боты против мошенников

25 января 2017 года в 12.40 в женской общине в честь Святых жен-мироносиц с. Клыкова Козельской епархии произошел пожар.

Более 50 мошенников объявили в Сети о сборе средств



Противодействие:

- Бот «Совесть»
- Встречная атака
- «Бот-юрист»

ЧТО ДЕЛАТЬ?

- **Люди** – Обучить
 - **Процессы** - Настроить
 - **Технологии** – Внедрить
-
- Спецназ информационной войны
 - Кибероружие

Что почитать: Forbes Russia N2, 2015 и др.



Разведка сетью: как система Avalanche помогает спецслужбам и бизнесу

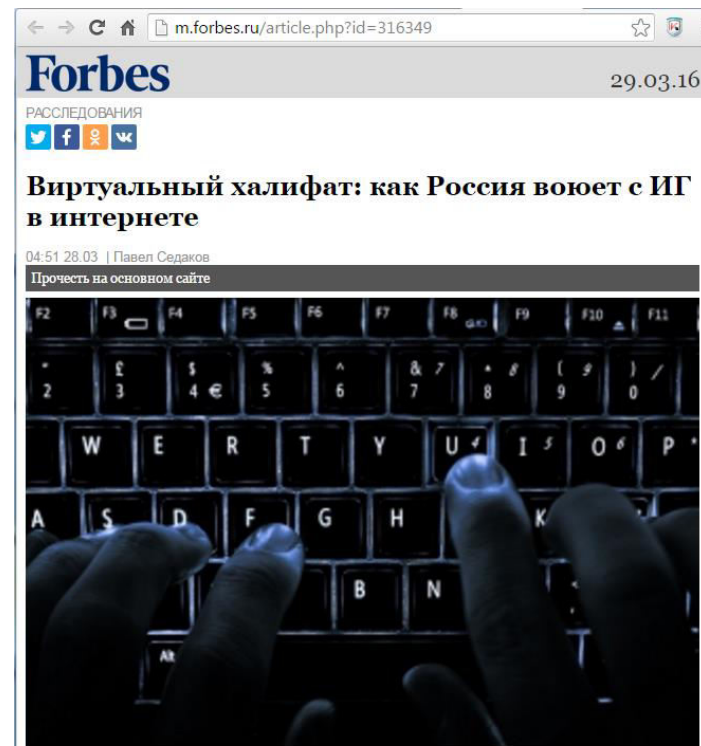


Фото Сергея Мельникова для РГТВ

Подполковник спецслужб в отставке Андрей Масалович создал программу Avalanche для борьбы с сетевыми угрозами. За что власти и корпорации ценят разработку?

«Русские, вперед!» — десятку лидеров в масках высказывают двери торгового центра «Бирюза» в Бирюлево. Из разбитых окон валит дым, в полицейских летят бутылки и камни. Предотвратить погром, которым закончился 13 октября 2013 года народный сход, силовики не смогли, хотя информация о нем была. «За три часа до начала беспорядков у меня в ноутбуке застряла красная лампочка — сигнал тревоги. — вспоминает 53-летний Андрей Масалович, президент корпорации «Информус» и разработчик поисково-аналитической системы Avalanche. — Мы заметили, что в группе «Суровое Бирюлево» в соцсети и на ресурсе «Я-Русский» началась прямая координация протестов».

После событий в Бирюлево систему рыночного предупреждения на базе Avalanche — «Лампа Пуле» — использовали в МВД в управлении оперативно-разыскной информацией (УОРИ). От государства не отстает и бизнес — банки и



Виртуальный халифат: как Россия воюет с ИГ в интернете

04:51 28.03 | Павел Седаков

Прочсть на основном сайте



К борьбе с исламистами подключаются частные компании: они отслеживают вербовщиков, блокируют электронные кошельки и следят за перепиской в офисах

В феврале 2015 года Андрей Масалович, экс-подполковник ФАПСИ и создатель поисково-аналитической системы *Avalanche*, прилетел в Казань: здесь его ждало дело государственной важности. Через четыре месяца республика принимала Международный чемпионат по водным видам спорта. Спецслужбы

Преимущества технологии Avalanche:

Обучение пользователей

- Учебный курс «**Конкурентная разведка в Интернете**» - 2 дня
- Учебный курс «**Информационная безопасность в Интернете**» – 3 дня
- Учебный курс «**Технологии информационного противоборства в Интернете**» – 2 дня

Спасибо за внимание 😊

Неверова Дарья Владиславовна

- ❑ E-mail: Dneverova@infosystem.ru
- ❑ Phone: +7 (495) 120-04-02

Масалович Андрей Игоревич

- E-mail: avalanche100500@gmail.com
- Phone: +7 (964) 577-2012

iam.ru/tipaguru.htm

